

Status of the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously Presented) A method comprising:

receiving, using a processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures computational resources for accessing electronic data;

determining, using the processing device, whether access candidate attributes satisfy access requirements of the resources, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited;

granting, using the processing device, access to the first security level based on a determination indicating that access to the first level is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures the electronic data;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data secured by the second security level;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the access requirements of the electronic data in response to a determination indicating that access to the second security level is prohibited; and

in response to obtaining the authorization from the resolution authority, granting the access candidate access to the second security level.

2. (Previously Presented) The method of Claim 1, further comprising granting access to the second security level in response to determining that the access candidate attributes satisfy the access requirements of the electronic data.

3. (Previously Presented) The method of Claim 1, further comprising denying access to the second security level if the authorization for the second request cannot be obtained.
4. (Previously Presented) The method of Claim 1, wherein at least one of the access requirements of the resources and the access requirements of the electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to a controller via a network.
5. (Previously Presented) The method of Claim 1, wherein at least one of the access requirements of the resource and the access requirements of the electronic data comprise a citizenship status of the access candidate or a current location of the access candidate.
6. (Previously Presented) The method of Claim 5, wherein the access candidate attributes comprise a citizenship status of the access candidate or a current location of the access candidate.
7. (Previously Presented) A method comprising:
 - receiving, using a processing device, a first request, from a first sponsor of an access candidate, for physical access to a computer network;
 - determining, using the processing device, whether access candidate attributes satisfy access requirements of physical access, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that physical access is prohibited;
 - granting, using the processing device, the physical access to the computer network based on a determination indicating that physical access is not prohibited;
 - receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to electronic data in the computer network in response to the granting of physical access to the computer network;
 - determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy access requirements of the electronic data in response to a determination indicating that access to the electronic data is prohibited; and
in response to obtaining the authorization from the resolution authority, granting the access candidate access to the electronic data.

8. (Previously Presented) The method of Claim 7, further comprising granting access to the electronic data in response to a comparison of the access candidate attributes with the access requirements of the electronic data indicating that access to the electronic data is not prohibited.

9. (Previously Presented) The method of Claim 7, further comprising denying access to the electronic data if the authorization for the second request cannot be obtained.

10. (Previously Presented) The method of Claim 7, wherein the access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

11. (Previously Presented) The method of Claim 7, wherein at least one of the access requirements of the electronic data and the access requirements of physical access comprise a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

12. (Previously Presented) The method of Claim 11, wherein the access candidate attributes comprise an existence of a data access agreement; a current location of the access candidate; or a citizenship status of the access candidate.

13. (Previously Presented) The method as in Claim 7, wherein at least one of the access requirements of the electronic data and access requirements of physical access comprise a current location of the access candidate or a citizenship status of the access candidate.

Reply to Office Action of October 7, 2011

14. (Previously Presented) The method of Claim 7, wherein at least one of the request for physical access or the request for access to the electronic data is submitted by more than one sponsor of the access candidate.

15. (Previously Presented) A method comprising:

identifying, using a processing device, a plurality of data subsets of electronic data, wherein respective data subsets correspond to respective sets of access requirements;

determining, using the processing device, at least one data class associated with the respective data subsets, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the at least one data class;

receiving, using the processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures physical access to a computer workstation for accessing the electronic data, the first request including access attributes of the access candidate comprising an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited;

granting, using the processing device, access to the first security level based on a determination indicating that access to the first security level is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures access to at least one of the plurality of data subsets;

determining, using the processing device, whether the access candidate attributes satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets in response to a determination indicating that access to the at least one of the plurality of data subsets is prohibited; and

in response to obtaining the authorization from the resolution authority, granting the access candidate access to the second security level.

16. (Previously Presented) A system comprising:

storage means for receiving and storing electronic data using a computer network;

means for evaluating a first request for access to one or more resources in the computer network, wherein the resources secure the electronic data, wherein an evaluation of the first request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the resources, and wherein the one or more attributes of the access candidate are revisable if the first comparison indicates that access is prohibited;

means for granting access to the one or more resources if the first comparison indicates that access is not prohibited;

means for evaluating a second request for access to the electronic data by the one or more resources, wherein an evaluation of the second request includes a second comparison of the one or more attributes of the access candidate with one or more access requirements associated with the electronic data;

means for obtaining authorization for the second request from a resolution authority if the one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the electronic data in response to the evaluation of the second request indicating that access to the electronic data is prohibited; and

means for granting, in response to obtaining the authorization from the resolution authority, the access candidate access to the electronic data using the one or more resources.

17. (Previously Presented) The system of Claim 16, further comprising means for granting access to the electronic data using the one or more resources configured to access and manipulate the electronic data if the second comparison indicates that access to the electronic data is not prohibited.

18. (Previously Presented) The system of Claim 16, wherein the access candidate is denied access to the electronic data if the authorization for the second request cannot be obtained.

19. (Previously Presented) The system of Claim 16, wherein the one or more access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

20. (Previously Presented) The system of Claim 16, wherein at least one of the one or more access requirements associated with the recourses and the one or more access requirements associated with the electronic data relates to at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; or a citizenship status of the potential access candidate.

21. (Previously Presented) The system of Claim 20, wherein the one or more access candidate attributes relates to at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

22. (Previously Presented) The system of Claim 16, wherein the one or more access requirements associated with the electronic data includes at least one of a current location of the access candidate or a citizenship status of the access candidate.

23. (Previously Presented) A system comprising:

storage configured to receive and store electronic data using a computer network;
one or more resources configured to process and manipulate the electronic data using a computer network;

a resource access controller configured to grant access to one or more resources, in response to a request for access to the one or more resources, based at least in part on a comparison of a citizenship status and a current location of an access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement are associated with the one or more resources;

one or more data access controllers configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison of the citizenship status and the current location of the access candidate with the citizenship requirement and the location requirement associated with the one or more data classes of the corresponding portion of the electronic data;

one or more resolution authorities configured to:

modify access requirements associated with the one or more data classes,
and

authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller indicating that access is prohibited; and

a data access module configured to:

evaluate a request for access to one or more portions of the electronic data using the one or more resources,

identify one or more data access controllers corresponding to the one or more portions of the electronic data, and

forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data.

24. (Previously Presented) A method comprising:

receiving, using a controller in a computer network associated with secured electronic data, a request for access to the secured electronic data in the computer network;

comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data;

obtaining authorization for the request from a resolution authority if one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the secured electronic data; and

in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information,

wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data.

25. (Previously Presented) The method of Claim 24, further comprising granting access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited.

26. (Previously Presented) The method of Claim 24, wherein the one or more access requirements associated with the secured electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to the controller via a network.

27. (Previously Presented) The method of Claim 24, wherein the one or more access requirements associated with the secured electronic data are related to at least one of a citizenship status or a current location of the access candidate.

28. (Previously Presented) The method of Claim 27, wherein the one or more attributes of the access candidate include at least one of a citizenship status or a current location of the access candidate.

29. (Previously Presented) A method comprising:

receiving, using a controller in a computer network associated with secured electronic data in the computer network, a request for access to the secured electronic data in the computer network;

comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data;

granting, using the controller, access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited;

obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited; and

in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information,

wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data.

30. (Previously Presented) An article of manufacture including a non-transitory computer-readable medium having instructions stored thereon, execution of which causes a processing device to perform operations comprising:

receiving, using a processing device, a request for access to a first security level in a computer network;

comparing, using the processing device, one or more attributes of an access candidate with one or more access requirements associated with the first security level, wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination indicating that access by the access candidate to the first security level is prohibited;

granting, using the processing device, access to the first security level based on a comparison indicating that access by the access candidate to the first security level is not prohibited;

receiving, using the processing device, a request for access to a second security level in the computer network;

obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited.

31. (Previously Presented) The article of manufacture of Claim 30, further comprising granting access to the second security level in response to a comparison of the one or more attributes of the access candidate with the one or more access requirements associated with the second security level indicating that access to the second security level by the access candidate is not prohibited.

32. (Previously Presented) The article of manufacture of Claim 30, further comprising denying access to the second security level if the authorization for the request cannot be obtained.

33. (Previously Presented) The article of manufacture of Claim 30, wherein the one or more attributes of the access candidate is represented as part of a graphical display associated with the access candidate and accessed for display via a network.

34. (Previously Presented) The article of manufacture of Claim 30, wherein the one or more access requirements associated with the first security level relates to at least one of: a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

35. (Previously Presented) The article of manufacture of Claim 34, wherein the one or more attributes of the access candidate relates to at least one of: an indication of whether the access candidate has a data access agreement; a current location of the access candidate; or a citizenship status of the access candidate.

36. (Previously Presented) The article of manufacture of Claim 30, wherein the one or more access requirements associated with the second security level relates to at least one of a current location of the access candidate or a citizenship status of the access candidate.

Reply to Office Action of October 7, 2011

37. (Previously Presented) The article of manufacture of Claim 30, wherein at least one of the request for access to the first security level or the request for access to the second security level is submitted by one or more sponsors.
38. (Previously Presented) The method as in claim 1, further comprising granting a waiver of the access requirements.
39. (Cancelled)
40. (Cancelled)
41. (Previously Presented) The method of claim 1, further comprising receiving supplemental evidence verifying the access candidate attributes.
42. (Previously Presented) The system of claim 15, wherein the data subsets are separated into the at least one data class based on a data provider of the data.
43. (Previously Presented) The method of claim 15, wherein the physical access comprises physical access to a facility housing the computer workstation.
44. (Previously Presented) The method of claim 15, wherein the physical access comprises logging on to the computer workstation.